Chain-C Software Design Specification
for the
Generation-3
Personnel Safety System
(PSS)
of the
Advanced Photon Source
at
Argonne National Laboratory
9700 Cass Avenue
Argonne, Illinois 60439

WBS x.1.4.1.4.30.1

Approved By:

_____	**_____**
John Carwardine, Associate Division Director, ASD	Date
_____	**_____**
xxxxxxxxxx, Group Leader, SI, ASD	Date
_____	**_____**
Mohan Ramanathan, Chairman, Adhoc Generation 3 committee	Date
_____	**_____**
Jim Lang, Radiation Safety,	Date

Prepared By:

_____   _____
John Servino,   Date
SI, ASD

Reviewed By:

_____   _____
Roy Emerson,   Date
SI, ASD

_____   _____
Jon Hawkins,   Date
SI, ASD

_____   _____
Martin Knott,   Date
ESS, ASD

_____   _____
Mike Fagan,   Date
SI, ASD

_____   _____
Nick Friedman,   Date
SI, ASD

NOTIFICATION OF SPECIFICATION REVISIONS

(INDEX)   **INDEX OF PAGE REVISIONS**

PAGE NO.	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
REV. NO.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

PAGE NO.	16	17	18	19	20	21	22	23	24						
REV. NO.	00	00	00	00	00	00	00	00	00						

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

PAGE NO.															
REV. NO.															

REVISION AUTHORIZATION

REVISION NUMBER	00	01	02	03	04	05	06	07	08
DCN NUMBER									
DATE									
APPROVED BY									

ANL-309 (12-83)

Table of Contents

1. Introduction

1.1 Purpose

This Software Design Specification presents the requirements to be use to develop the software for the Personnel Safety System (PSS). This concept is to be use by the programmer to develop the code for the Chain-C Command and Control Programmable Logic Controller.

1.2 Definitions, acronyms, and abbreviations

The following are some of the frequently appearing or unique acronyms used in this document.

Down Stream: The direction defined by the path from the Storage Ring to the end of the last Station of a beam line. The beam flow is from the Storage Ring through the Front End Shutters into and through Station A and then to Station B and so on until the beam encounters either a closed Shutter or a beam stop at the end of the last Station.

Up Stream: The direction defined by the path from the end of last Station of a beam line to the Storage Ring.

Beam Active: Based on shutter position the system can determine if there is Active Beam in a Station.
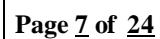Ex-1: If the Front End Shutters are closed, No Station can be Beam Active.
Ex-2: If the Front End Shutters are open then Station-A is Beam Active.
Ex-3: If the Front End Shutters are open and the downstream shutters are open, then Station-A is Beam Active and the down stream Stations are Beam Active

ACIS	Accelerator Control and Interlock System
APS	Advanced Photon Source
ASD	Accelerator Systems Division
BLEPS	Beamline Equipment Protection System
C&C	Command and Control system
CPU	Central Processing Unit
DOE	Department of Energy
ES&H	Environment, Safety & Health Manual
EPICS	Experimental Physics and Industrial Control System
EPS	Equipment Protection System
ESD	Emergency Shut Down System
FES	Front End Shutters.
FEEPS	Front End Equipment Protection System
I/O	Input Output
PSS	Personnel Safety System
PLC(s)	Programmable Logic Controller(s)
SAD	Safety Assessment Document
SLAC	Stanford Linear Accelerator Center
SRS	Software Requirements Specification
TBD	To Be Defined/Decided
XFD	Experimental Facilities Division

1.3 Scope

This Software Design Specification is limited to the Generation-3 PSS Chain-C Command & Control System. For requirements specific to an individual Beamline, refer to the User Software Requirements Specification.

1.4 Revision Record

Revision	Dated	Comments
-00	03/19/04	Create Document

2. Applicable Documents

The following documents of the exact issue shown form a part of this specification to the extent specified herein. In the event of conflict between the documents referenced herein, and the contents of this specification, the contents of this specification shall supersede requirement.

2.1 Government Documents

- DOE ORDER 420.2, November 05,1998
- Accelerator Safety Implementation Guide for DOE O 420.2, Draft, May 1, 1999
- DOE ORDER 5480.25, November 03, 1992
- DOE GUIDANCE 5480.25, September 1, 1993

2.2 Non-Government Documents

- APS Safety Assessment Document(SAD), Rev 1, May 1998, Argonne National Laboratory, Argonne, IL
- Argonne National Laboratory Environment, Safety & Health Manual(ES&H), May 27, 1999
- SLAC Report 327, April 1988, Stanford Linear Accelerator Center, Menlo Park, CA
- NCRP Report No. 88, Issued 30 December 1986, National Council on Radiation Protection
- Document No. 1111-00001-00 APS Quality Assurance Plan, dated May 1990

2.3 APS Standard

- Software Coding Standards for the Personnel Safety System of the APS.

2.4 PSS Specifications

- System Requirements Specification for the Generation-3 PSS
- Functional Description for the Generation-3 PSS
- Beamline Requirement Document
- Chain-C Master Input/Output Listings for the Generation-3 PSS Beamlines
- Chain-C Master Fault Listings for the beamline Generation-3 PSS

2.5 Other Publications

- Allen Bradley Control Logic PLC Programming Manuals
- Rockwell RSLogix5000 Programming Software Manuals

3. Operational Concepts

3.1 Overview

The PSS shall consist of two redundant Emergency Shut Down (ESD) subsystems and a separate command and Control (C&C) subsystem (see system constrains 2.5.1.2 & 2.5.1.3), which in turn interface with systems that control other aspects of the facility. The following block diagram shows the relationships between the major subsystems within PSS and its relationship to the other systems.
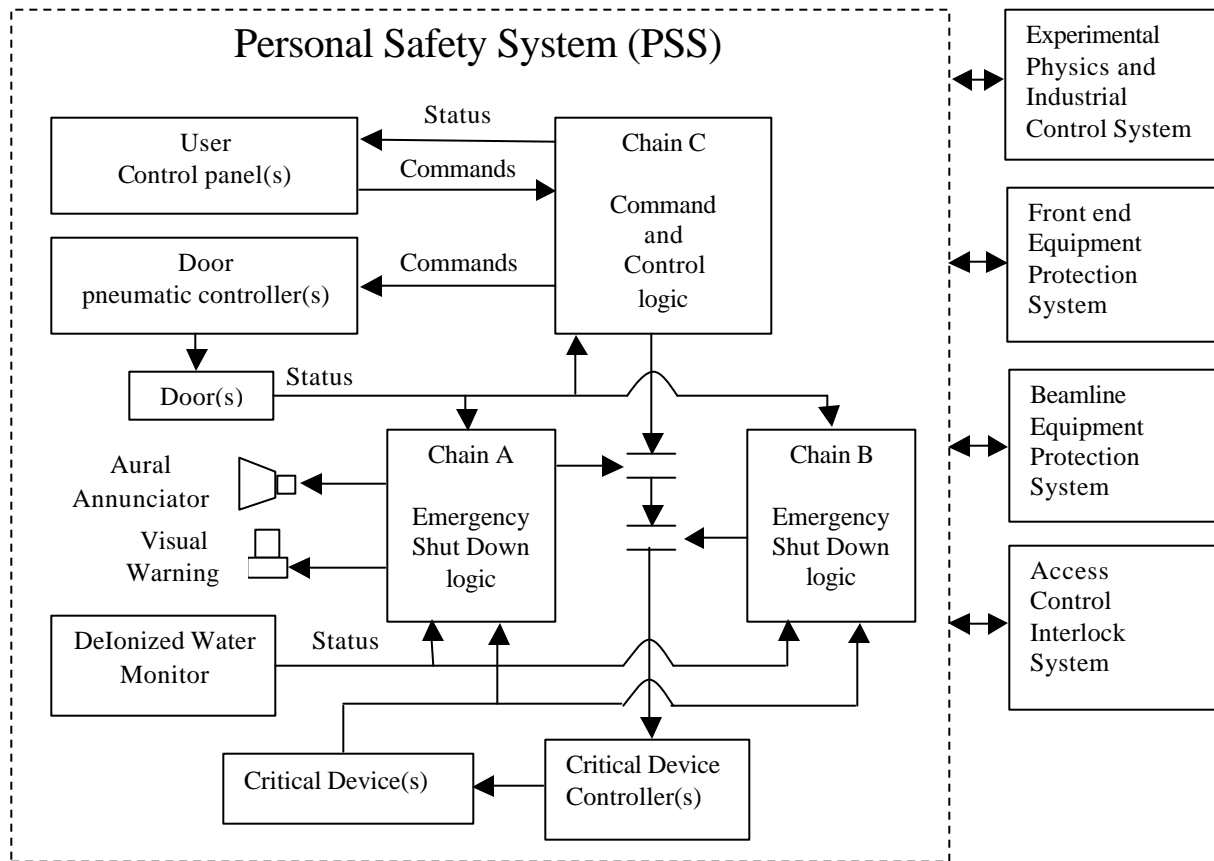
Hardware Interface Diagram

3.2 Rationale

The PSS system is a system of permits or enables that allow the safe use of an experimental station. Three PLCs from different manufacturers are used to minimize the likelihood that a hardware defect or a programming software package defect would be common to all three and cause simultaneous unsafe operation. The input to the PLCs is through independent sensors and wiring to eliminate the possibility that a single sensor or wire failure will cause improper operation. The output of the PLCs are in series requiring all have to be in an agreement for operation of critical devices. Additionally, three different programmers are used to implement the control code used in the Chain-A, Chain-B and Chain-C PLCs to minimize the chance of propagating a human error from one system to the others.

4. Program Design General

4.1 Chain-C Programming Environment

RSLogix-5000 and RSNetworks by Rockwell Software will be the software tool for programming, configuring and testing the Chain-C system.

4.2 Chain-C Programming Language

The Chain-C Control Logix System will be programmed in Ladder Logic and/or Structured Text.

5. Program Design Details

This section contains a narrative for the Chain-C control.

5.1 Chain-A & Chain-B to Chain-C Communications

Chain-A & Chain-B will transmit specific configured signals to Chain-C for status and control. These includes the following:

- All Inputs
- All Outputs
- All Faults, including Time and Date Stamp
- Specific status signals

5.2 Fault handling

Any Chain-A / Chain-B Major or Minor Fault, or Chain-C Minor fault will sequence close all shutters and inhibit them from opening until all the Faults are cleared.
Chain-C Warning will not close any shutters.

6. Mezzanine - General

This section describes the mezzanine functions and interfaces.

6.1 Watch Dog From Chain-A

The program monitors the Chain-A 1-Hz pulse.

This signal determines whether the Chain-A controller is communicating and functioning.

- When the watchdog fails a Minor Fault is generated.

6.2 Watch Dog From Chain-B

The program monitors the Chain-B 1-Hz pulse.

This signal determines whether the Chain-B controller is communicating and functioning.

- When the watchdog fails a Minor Fault is generated.

6.3 CPU Key Switch

The key switch is in not Run Position; it is in Remote Run or Program mode.

- This will generate a Minor Fault.

6.4 PLC Battery

The CPU's backup battery prevents the lost of its memory in the case of power failure.

- When the battery is disconnected or its power is below operating range. The program will generate a warning.

6.5 PLC Force Present

The Chain-C PLC internally detects a force is present.

- These will generate a Minor Fault.

6.6 Remote I/O Loss of Communication

There is a loss or interruption of communications to the Remote I/O Racks.

- These will generate a Minor Fault.

6.7 Chain-C 24Vdc Power Supplies Active/OK

This monitors the Chain-C 24Vdc Field Device / Strobes & Locks and HMI power supplies.

- When a Power Supply fails, a Minor Fault is generated.

6.8 Mezzanine Test Connector Box Open

This monitors the Test Connector Box interface.

- When this signal transitions from ON to OFF, a Minor Fault is generated.

6.9 Chain-C Disable All Outputs

This signal is sent from the Validation Testing.

- When this signal is ON, the program disables all of the Chain-C Outputs.

6.10 Tunnel Test Connector Box Open

This monitors the Tunnel Test Connector Box interface.

- When this signal transitions from ON to OFF, a Minor Fault is generated.

6.11 Chain-C Fault Present To Chain-A

When a Chain-C or Chain-B fault is active, this signal will be sent to Chain-A for the following:

- Inhibit the start of Search & Secure sequence for any Station.
- Abort any non-completed Search & Secure sequences for any Station.
- This signal will not abort any completed Search & Secured Stations

7. Mezzanine - Front End Shutter-General

7.1 ACIS Global-Online

Utilized as a Front End Shutter Permit

- Beam Active:
  When this signal transitions from ON to OFF, a Minor Fault is generated

- Other conditions:
  If this signal is OFF, the program will not allow the FES to open.
  If this signal is ON, it will be used as one of the permits that allows the FES to open.

7.2 ACIS Shutter Permit

Utilized as a Front End Shutter Permit

- Beam Active:
  When this signal transitions from ON to OFF, the FES will sequence close.

- Other conditions:
  If this signal is OFF, the program will not allow the FES to open.
- If this signal is ON, it will be used as one of the permits that allows the FES to open

7.3 FEEPS Shutter Permit

Utilized as a Front End Shutter Permit

- Beam Active:
  When this signal transitions from ON to OFF, the FES will sequence close.

- Other conditions:
  If this signal is OFF, the program will not allow the FES to open.
- If this signal is ON, it will be used as one of the permits that allows the FES to open

7.4 FE Shutter Disable Confirm (<3psi)

FES pressure feedback air valve. This is a "LOW" true signal.
It indicator that there is Less Than 3 PSI in the air valve.
This signal is integrated with Global Online.

- Global Online = ON: and this signal is ON, a Minor Fault is generated.

- Global Online = OFF: and this signal is OFF, a Minor Fault is generated.

7.5   FE Shutter Pressure (>60psi)

FES pressure feedback air valve.
It indicator that there is Greater Than 60 PSI in the air valve.
This signal is integrated with Global Online.

- Global Online = ON: and this signal is OFF, a Minor Fault is generated.

- Global Online = OFF: and this signal is ON, a Minor Fault is generated.

8. Mezzanine - Front End Shutter-Status/Control

The Chain-A & Chain-B FES position limit switch inputs are sent to Chain-C.
These switches are used to determine the status/position of the FES.
The FES information is integrated throughout the C&C system for status, control and fault detection.

8.1 FES Position Switches

- Photon Stop-1 Opened Limit Switch
- Photon Stop-1 Closed Limit Switch
- Photon Stop-2 Opened Limit Switch
- Photon Stop-2 Closed Limit Switch
- Safety Stop-1 Opened Limit Switch
- Safety Stop-1 Closed Limit Switch
- Safety Stop-2 Opened Limit Switch
- Safety Stop-2 Closed Limit Switch

8.2 FES Cylinder Faults

Each of the Chain-A & Chain-B Shutter Cylinder can generate up to five faults per chain.
This is based on the position of the Chain-A & Chain-B limit switch inputs and the Chain-C open command status. The following is an example of the fault for PS-1 Chain-A.

- Chain-A PS-1 Close Switch Fail
- Chain-A PS-1 Open Switch Fail
- Chain-A PS-1 Both Switch
- Chain-A PS-1 Close Command Fail
- Chain-A PS-1 Open Command Fail

8.3 FES Open/Close Commands

Chain-C will always sequence open and sequence closed the FES cluster.
When the output is energized the cylinder is being commanded open.
When the output is de-energized the cylinder is being commanded close.

- Photon Stop-1 Open Command
- Photon Stop-2 Open Command
- Safety Stop-1 Open Command
- Safety Stop-2 Open Command

8.3.1 FES PS-1 Operation

The FES PS-1 Cylinder can operate independently of the FE Cluster.
A signal from the FEEPS system can open or close the PS-1 cylinder.
A Major Fault will over ride all open commands and the close PS-1 cylinder.

- When the FEEPS PS-1 Open Request is active and there are no Major Faults present, the PS-1 Cylinder will be commanded to open.

- When the FEEPS PS-1 Open Request is inactive and the FES (PS-2, SS-1 SS-2) has not been commanded open or is closed, the PS-1 Cylinder will be commanded to close.

8.3.2 FES Open Sequence

1. All conditions are satisfied for FES operation.
2. SS-1 and SS-2 will be commanded open.
3. The Chain-A & Chain-B SS-1 and SS-2 Opened Limit Switches are confirmed open for one second.
4. PS-1 and PS-2 will be commanded open
5. The Chain-A & Chain-B PS-1 and PS-2 Opened Limit Switches are confirmed open for one second.
6. PS-1, PS-2, SS-1 and SS-2 are confirmed open.

8.3.3 FES Close Sequence-(PS-1 was already open by FEEPS)

1. The PS-2 open command is removed.
2. If PS-2 does not close in three seconds, PS-1 will be commanded to close.
3. The Chain-A & Chain-B PS-1 or PS-2 Opened Limit Switches are confirmed closed for one second.
4. The SS-1 and SS-2 open command is removed.
5. The Chain-A & Chain-B S-S1 and SS-2 Opened Limit Switches are confirmed open for one second.
6. PS-2, SS-1 and SS-2 are confirmed closed.

8.3.4 FES Close Sequence-(PS-1 was not opened by FEEPS)

1. The PS-1 and PS-2 open command is removed.
2. The Chain-A & Chain-B PS-1 or PS-2 Opened Limit Switches are confirmed closed for one second.
3. The SS-1 and SS-2 open command is removed.
4. The Chain-A & Chain-B SS-1 and SS-2 Opened Limit Switches are confirmed open for one second.
5. PS2, SS1 and SS2 are confirmed closed.

9. Station - General

This section describes the Station functions and interface.

9.1 Station User Key Enabled

This is a maintained signal used as a shutter permit for a critical section.

- If this signal is OFF, the shutter protecting that station is commanded to close.

- If this signal is ON, the shutter, protecting that station, will use this as one of the permits to allow the shutter to open.

9.2 Station APS Key Enabled

This is a latched/toggled signal used as a shutter permit for a critical section.

- If this signal is OFF, the shutter protecting that station is commanded to close.

- If this signal is ON, the shutter, protecting that station, will use this as one of the permits to allow the shutter to open.

- The latched APS interlock is sent to Chain-A & Chain-B.

9.3 Major Reset Key Switch

This key will reset only Major Faults when conditions are satisfied.
This signal is not used in Chain-C.

9.4 Minor Reset Key Switch

This key will reset only Minor Faults and Warning when conditions are satisfied.

9.5 Station Test Connector Box Open

This monitors the Station Test Connector Box interface.

- When this signal transitions from ON to OFF, a Minor Fault is generated.

9.6 Station Key Click and Error Buzz

These audible signals are used to alert the user of the status of their request from the HMI panel. Ex: Open Shutter Push Button.

- When a user command can be processed the Key Click audible will alert.

- When a user command can not be processed the Error Buzz audible will alert.

10. Station - Shutter Control

10.1 Shutter Operation

When the Open Shutter Push Button is pressed on the HMI panel, the shutter will be commanded open. The criteria for permitting a shutter to open changes based on shutter type and location. Specific shutter require sequencing, others do not. Refer to the Beamline Requirement Document for specifics.

The following is an example of the permits required for opening the FES, Station-A only.

- Chain-A Station-A is Beam Ready signal to Chain-C

- Chain-B Station-A is Beam Ready signal to Chain-C

- The are no Major or Minor Faults

- Station-A User Key is captured

- Station-A APS is enabled

- Station-A doors are closed and locked

- All FES Permits, Global On-line, ACIS, FEEPS, BLEPS, Pressures Switches, etc.

The Shutter will be commanded close when:

- The Close Shutter Push Button is pressed on the HMI panel

- Any Shutter Permit is disabled/removed

- Any Fault occurs

The Shutter Position Status (Open/Close) will be sent to BLEPS.

11. Station - Shutter-Status/Control Signals

The Chain-A & Chain-B FES position limit switch inputs are sent to Chain-C.
These switches are used to determine the status/position of the Station Shutters.
The Station Shutter information is integrated throughout the C&C system for status, control and fault detection.
Station Shutter can consist or two, three or four cylinder shutters

11.1 Position Switches

- Photon Stop Opened Limit Switch
- Photon Stop Closed Limit Switch
- Safety Stop Opened Limit Switch
- Safety Stop Closed Limit Switch
- Mono Stop-1 Opened Limit Switch
- Mono Stop-1 Closed Limit Switch
- Mono Stop-2 Opened Limit Switch
- Mono Stop-2 Closed Limit Switch

11.2 Shutter Cylinder Faults

Each of the Chain-A & Chain-B Shutter Cylinder can generate up to five faults per chain.
This is based on the position of the Chain-A & Chain-B limit switch inputs and the Chain-C open command status. The following is an example of the fault for MS-1 Chain-B.

- Chain-B MS-1 Close Switch Fail
- Chain-B MS-1 Open Switch Fail
- Chain-B MS-1 Both Switch
- Chain-B MS-1 Close Command Fail
- Chain-B MS-1 Open Command Fail

11.3 Shutter Open/Close Commands

Chain-C will always sequence open and sequence closed the shutter cluster if necessary.
Refer to FES operation.
When the output is energized the cylinder is being commanded open.
When the output is de-energized the cylinder is being commanded close.

- Photon Stop Open Command
- Safety Stop Open Command
- Mono Stop-1 Open Command
- Mono Stop-2 Open Command

12. Mode Shutter - Optional

The mode shutter controls will let the user configure the positioning of a mode shutter. Mode shutters have two operating positions. The Mode shutter may be put into a Mono mode or into a Non-Mono mode. The Non-Mono mode may also be identified as white or pink mode.

The Non-Mono mode is used to lock the shutter open to pass to the down stream stations a high intensity beam. This mode effectively creates a much larger experimental area for high intensity beam. This area extends down stream until a high intensity beam stop is encountered by the beam. This type of beam stop is normally referred to as a white beam stop. Notice that when in this mode, the area that must be protected by the PSS using the Front End Shutters as the critical device is increased.

The Mono mode is used when the user desires to contain the high intensity beam in the First Optical Enclosure (FOE). When in the Mono mode the mode shutter may be opened and closed by use of the shutter controls on the User Control Panel to control the passage of low intensity monochromatic beam to down stream stations.

12.1 Kirk Key Interlocks and Mode Selection

The following is and example of how a mode shutter is configured.

1. Reset any beam line faults that may be present.
2. Move all Kirk Keys to the Shutter Device Kirk locks and turn them to retract the lock plungers.
3. This will cause a device reset allowing mode selection to take place.
   A Mode Shutter Reset signal will be sent to Chain-A & Chain-B.
4. Push the Mono or Non-mono push button located on the electrical interface enclosure attached to the shutter table to select a mode.
5. The Non-mono indicator located on the HMI will flash when the Non-mono push button is pushed and the shutter assumes the Non-mono position.
6. The Mono Mode indicator located on the HMI will flash when the Mono push button is pushed and the shutter assumes the Mono position.
7. Move appropriate keys back to Mode Controller Panel.
8. The selected Mode (Mono or Non-mono) LED will be flashing.
9. Insert the Mode Select Key into the Key Switch on the Mode Control Panel and turn it to lock in the selected mode.
   A Mode Selected signal will be sent to Chain-A & Chain-B.
10. The selected Mode (Mono or Non-mono) indicator located on the HMI will now remain continuously on to indicate the shutter mode.
11. Remove the Mode Select Key from the panel.
12. This completes mode selection.

13. Station Door - Status/Control

There are two types of doors that are controlled by Chain-C.

- Manual doors: Lock / Unlock control, status and fault detection.

- Pneumatic doors: Complete door open/close/lock/unlock control, status and fault detection.

Note:
When a Fault is present, Manual and Pneumatic doors can be opened/unlocked when the beamline is Global-Offline, the FES Pressures Switches have transitioned and the FES are confirmed closed, not opened and all open commands are off.

13.1 Station Manual Door Control

Via the HMI Panel, a Manual Door can be locked or unlocked.

- Manual Doors can be unlocked when there is no beam in the Station and it is in a safe mode (Refer to the Beamline Requirement Document for specifics).

- Manual Doors can be locked when the Station is Searched and Secured.

13.2 Station Pneumatic Door Control

Pneumatic Door Close:
Pneumatic Door will close when the Door Close Button is pressed on the Door Control Panel. This button must be held until the door is confirmed closed. If the button is let go before the door is completely closed it will re-open. Once the door is confirmed closed it will lock the door.

Pneumatic Door Open:
Pneumatic Door will be permitted to open when there is no beam in the Station and it is in a safe mode (Refer to the Beamline Requirement Document for specifics). The door will be controlled open by the following

- The Door Open Button is pressed on the Door Control Panel

- The Emergency Egress Door Open Button inside the Station.

13.3 Station Door Closed Sensor

The Chain-A & Chain-B Door Closed Limit Switch Inputs are sent to Chain-C.
These switches are used to determine the status/position of the Station Doors.
The door switches are integrated throughout the C&C system for status, control and fault detection.

- Station door switch:

    - Door is open if the input is OFF

    - Door is closed if the input is ON.

    - Status is displayed on the HMI and door control panel.

    - Generates a Minor Fault on the HMI, Door-X Close Failure.

13.4 Station Door Locked Sensor

The Door Locked Switch Inputs are used to:

- Determine and display the door lock status on the HMI.

- Generate a Warning on the HMI, Door-X Lock Failure.

13.5 Station Door Key Click and Error Buzz

These audible signals are used to alert the user of the status of their request from the door control panel. Ex: Open Door Push Button.

- When a user command can be processed the Key Click audible will alert.

- When a user command can not be processed the Error Buzz audible will alert.

14. Notes & Comments